Vraagtekst	Toelichting
6.1.1.a Op welke wijze is het College van B&W betrokken bij beveiliging?	Het College behoort actief informatiebeveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen. Dit is een BRP en een SUWI-eis. Besluit BRP artikel 6PUN art 90. Suwinorm B.01/C.01: Het betreft hier de zichtbare -dus gedocumenteerde- ondersteuning (mate waarin) door het College vanuit de Governance. Het College stelt bijvoorbeeld de informatiebeveiligingsdoelstellingen vast, blijft op de hoogte door actieve voortgangsrapportering middels periodieke rapportages.Zie ook hoofdstuk 6.1.1 van de BIG: Betrokkenheid van het College van B&W bij beveiliging van de BIG p.20Benodigde documentatieIn ieder geval verslagen van vergaderingen waarin het onderwerp Informatiebeveiliging aan de orde gekomen is. Daarnaast behoort het management voldoende budgetten ter beschikking te stellen die passen bij de jaarlijkse informatieplanning. Ze behoren actief het belang van informatieveiligheid uit te dragen.Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.
6.1.2.a Zijn de rollen van de CISO en het lijnmanagement beschreven waar het de coördinatie van de activiteiten voor informatiebeveiliging betreft?	Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit de verschillende delen van de organisatie met relevante rollen en functies. Dit is een SUWI-eis.Suwinorm: B.01 en B.04Informatieveiligheid steunt idealiter op controle technische functiescheiding (CTFS) waarbij onderscheid wordt gemaakt tussen lijnmanagement (beschikkend en uitvoerend) en CISO (intern beschikkend voor voorschrijven veiligheidsstandaarden, te vergelijken met een bedrijfsbureau) en de uitvoer van de activiteiten als zodanig. Stel vast of deze CTFS zo aanwezig is en ingericht is.Zie ook hs 6.1.2 van de BIG: Coördineren van beveiliging p.20Benodigde documentatieOverzicht van IB functies met taken, bevoegdheden en verantwoordelijkheden (formeel vastgesteld).Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.
6.1.3.a Zijn de beveiligingsrollen voor wat betreft informatiebeveiliging van de (lijn, proces, systeem) manager belegd?	Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd. Dit is een SUWI-eis.Suwinorm B.05: Gedocumenteerd (in de vorm van matrix) aanwezigheid van rollen en verantwoordelijkheden volgens de RACI-principes. Deze documentatie vormt het inrichtingsvoorschrift voor de Suwinet-applicatie(s). Bijvoorbeeld in de vorm van functiebeschrijvingen en taakopdrachten waarin wordt verwezen naar de matrix. RACI staat voor Responsible, Accountable, Consulted en Informed.AVG : artikel 37, lid 1 Zie ook hs 6.1.3. van de BIG: Verantwoordelijkheden p.20Benodigde documentatieVoor relevante rollen en functies behoren de eisen te zijn uitgewerkt in functie- dan wel taak omschrijvingen.Ongeacht de plaats in de organisatie is er altijd enige verantwoordelijkheid met betrekking tot veiligheid van informatie. Ieder proces en informatiesysteem dient een eigenaar te hebben.Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.
6.1.3.b Heeft uw gemeente een Functionaris Gegevensbescherming benoemd?	De functionaris voor de gegevensbescherming (FG) dient met deskundige kennis van gegevensbeschermingswetgeving en -praktijken de verwerkingsverantwoordelijke of de verwerker bij te staan bij het toezicht op de interne naleving van de AVG. De FG houdt binnen een organisatie toezicht op de toepassing en naleving van de AVG. Een gemeente is verplicht om een FG aan te stellen. De FG functioneert als een verlengstuk van de Autoriteit Persoonsgegevens. AVG : artikel 37, lid 1
6.1.4.a Is er een geïmplementeerd proces voor het goedkeuren van nieuwe ICT-voorzieningen?	Er behoort een goedkeuringsproces voor nieuwe ICT-voorzieningen te worden vastgesteld en geïmplementeerd. Het goedkeuringsproces is onafhankelijk van een oplossing on-site of in de cloud.AVG art 28 lid 3 onder bZie ook hs 6.1.4 van de BIG: Goedkeuringsproces voor ICT-voorzieningen p.21Benodigde documentatie:Autorisatieproces nieuwe IT voorzieningen.

6.1.5.a Is voor alle typen werknemers uitgewerkt of er een geheimhoudingsverklaring getekend moet worden bij aanstelling?	Eisen voor vertrouwelijkheid of voor een geheimhoudingsovereenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie behoren te worden vastgesteld en regelmatig te worden beoordeeld.Het ondertekenen van een individuele verklaring integriteit / tot geheimhouding of het afleggen van de ambtseed of belofte is een BRP en PUN eis.BRP: WBP 12, lid 2PUN: WBP 12, lid 2Zie ook hs 6.1.5 van de BIG: Geheimhoudingsovereenkomst p.21Benodigde documentatieGeheimhoudingsverklaringen in personeelsdossiers.
6.1.6.a Worden er contacten onderhouden in relatie tot informatiebeveiliging met relevante (overheids) organisaties?	Er behoren geschikte contacten met relevante (overheids)instanties te worden onderhouden.Zie ook hs 6.1.6 van de BIG: Contact met overheidsinstanties p.21Implementatie ondersteuningOrganisaties behoren procedures te hebben geïmplementeerd die beschrijven wanneer en door wie er met autoriteiten contact behoort te worden opgenomen (bijvoorbeeld politie, brandweer, toezichthouders) en hoe de vastgestelde informatiebeveiligingsincidenten tijdig behoren te worden gerapporteerd, indien het vermoeden bestaat dat er wetgeving is overtreden. Organisaties die via het internet worden aangevallen kunnen bijstand van externe partijen (bijvoorbeeld een leverancier van internetdiensten of een telecommunicatiebedrijf) nodig hebben om actie tegen de aanvaller te ondernemen. Overige informatie: Het onderhouden van dergelijke contacten kan een eis zijn voor het ondersteunen van het beheer van informatiebeveiligingsincidenten (13.2) of het bedrijfscontinuïteit- en noodplanproces (hoofdstuk 14). Benodigde documentatie In geval van een calamiteit dient duidelijk te zijn langs welke lijnen de communicatie dient te verlopen. Dit kan vastgelegd zijn in calamiteiten procedures, incident management en responsebeleid, noodplannen, Business Continuity Management (BCM).
6.1.7.a Onderhoudt de gemeente contact met relevante expertise groepen?	Er behoren geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden.Zie ook hs 6.1.7 van de BIG: Contact met speciale belangengroepen p.21Benodigde documentatie:Bevestigingsmail aansluiting bij IBDImplementatie voorbeelden:Het lidmaatschap van bepaalde belangengroeperingen of forums behoort te worden beschouwd als een middel om:a) kennis te vergroten van beproefde werkwijzen (‘best practice’) en op de hoogte te blijven van de laatste stand van zaken op het gebied van informatiebeveiliging;b) te waarborgen dat kennis en begrip van het vakgebied informatiebeveiliging volledig actueel en compleet zijn;c) vroegtijdig signalen te krijgen van waarschuwingen, adviezen en ‘patches’ die verband houden met aanvallen en kwetsbaarheden;d) toegang te verkrijgen tot deskundig informatiebeveiligingsadvies;e) informatie over nieuwe technologieën, producten, bedreigingen of kwetsbaarheden te delen en uit te wisselen; geschikte aanspreekpunten te leveren wanneer men te maken heeft met informatiebeveiligingsincidenten (zie ook 13.2.1).

6.1.8.a Wordt het informatiebeveiligingsbeleid minimaal jaarlijks onafhankelijk beoordeeld?	De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheerdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich wijzigingen voordoen in de implementatie van de beveiliging. Dit is een BRP en een SUWI-eis.Wet BRP 4.3, lid 1Suwinorm: C.01 en C.08De onafhankelijke beoordeling (resulterend in een transparantierapportage) zou moeten worden geïnitieerd door de directie. Een dergelijke onafhankelijke beoordeling is nodig om te waarborgen dat de organisatie een geschikte, toereikende en doeltreffende aanpak van het beheer van informatiebeveiliging hanteert. In de beoordeling behoren de mogelijkheden voor verbetering en de noodzaak om wijzigingen aan te brengen in de beveiligingsaanpak, waaronder het beleid en de beheersdoelstellingen, te worden meegenomen. Onafhankelijk betekent hier dat een beoordeling zou moeten worden uitgevoerd door personen die onafhankelijk zijn ten opzichte van de omgeving die wordt beoordeeld, bijvoorbeeld de interne auditor, een onafhankelijke manager of een derde partij die in dergelijke beoordelingen is gespecialiseerd, voor zover zij beschikken over de juiste vaardigheden en ervaring. Zie ook hs 6.1.8 van de BIG: Beoordeling van het informatiebeveiligingsbeleid p.21Benodigde documentatieAudit verslagen, gespreksverslagen, verslag van de beoordeling van het beleid.
Vraagtekst	**Toelichting**
6.2.1.a Worden externe partijen (inclusief samenwerkingsverbanden) gebruikt om ICT-voorzieningen in stand te houden dan wel te beheren of worden externe partijen gebruikt voor de invulling van bedrijfsprocessen?	De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend. De verwerker dient zo spoedig mogelijk, zonder onnodige vertraging, de inbreuk te melden aan de verwerkingsverantwoordelijke. Soms kan dit onverwijld in andere gevallen is onderzoek nodig om vast te stellen dat er een inbreuk is. De termijn van 24 uur is niet opgenomen in wetgeving en is niet maatgevend. Het format verwerkersovereenkomst van de IBD houdt hiervoor 48 uur aan. Het advies is om een concrete termijn op te nemen in de contracten met leveranciers. Aanvullend: de uren die nodig zijn om de inbreuk na constatering bij de verwerker richting de verantwoordelijke te doen worden niet in mindering gebracht bij de 72-uur termijn die geldt voor de melding richting de AP vanuit de verantwoordelijke.AVG art. 33, lid 1Deze vraag wordt gebruikt voor de routing op de vervolgvragen.
6.2.1.b Is er voor uitbesteding van een proces of systeem een risicoafweging gemaakt en zijn de relevante beveiligingsrisico's in kaart gebracht?	De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend.
6.2.1.c Als er uitbesteed is, zijn er dan beveiligingsmaatregelen vastgelegd in de (inkoop) contracten?	Er behoort te worden gewaarborgd dat de externe partij kennis draagt van zijn verplichtingen en verantwoordelijkheden die gepaard gaan met de toegang tot informatie en IT voorzieningen van de organisatie.
6.2.1.d Als er aan een leverancier is uitbesteed en het doel van de uitbesteding is het verwerken van persoonsgegevens, is er dan met de leverancier een (verwerkers)overeenkomst afgesloten?	De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling.
6.2.1.e. Kunt u aangeven op welke wijze de afspraken zijn gemaakt?	

6.2.1.f Als er persoonsgegevens worden verwerkt, waarbij er sprake is van een verhoogd risico, wordt er dan voorafgaand aan de start van de verwerking een data protection impact assessments (DPIA's) uitgevoerd?	Bij verwerking van persoonsgegevens, waarbij sprake is van een verhoogd risico, is het uitvoeren van data protection impact assesments (DPIA's) voorafgaand aan de start van de verwerking verplicht volgens de AVG. Alleen dan is de impact op de privacy juist in kaart gebracht.AVG Artikel 35 lid 1 1
6.2.1.g Is in deze contracten opgenomen dat een leverancier verplicht is om binnen 24 uur alle beveiligingsinbreuken te melden?	De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend. De verwerker dient zo spoedig mogelijk, zonder onnodige vertraging, de inbreuk te melden aan de verwerkingsverantwoordelijke. Soms kan dit onverwijld in andere gevallen is onderzoek nodig om vast te stellen dat er een inbreuk is. De termijn van 24 uur is niet opgenomen in wetgeving. De standaard verwerkersovereenkomst van de IBD houdt 24 uur aan. Aanvullend: de uren die nodig zijn om de inbreuk na constatering bij de verwerker richting de verantwoordelijke te doen worden niet in mindering gebracht bij de 72-uur termijn die geldt voor de melding richting de AP vanuit de verantwoordelijke.
6.2.1.h Worden de aan derden opgelegde informatiebeveiligingsmaatregelen jaarlijks gecontroleerd?	Als aan een leverancier beveiligingseisen worden opgelegd, dan moeten deze eisen/afspraken jaarlijks aantoonbaar geïmplementeerd zijn. Dit is een eis vanuit AVG/SUWI/BRP.
6.2.1.i Hebben u en/of uw externe softwareleveranciers bij softwareontwikkeling privacy by design ingericht?	Verwerkingsverantwoordelijken en verwerkers behoren niet meer persoonsgegevens te verwerken dan strikt noodzakelijk voor realisatie van het beoogde doel. Externe softwareleveranciers dienen deze eis uit de AVG te respecteren. AVG art 25.
6.2.1.j Heeft u privacy by default ingericht binnen uw processen en systemen?	Verwerkingsverantwoordelijken en verwerkers behoren niet meer persoonsgegevens te verwerken dan strikt noodzakelijk voor realisatie van het beoogde doel. Externe softwareleveranciers dienen deze eis uit de AVG te respecteren. AVG art 25.
6.2.1.k Heeft uw gemeente werkende procedures voor alle rechten van betrokkenen?	Onder de Algemene Verordening Gegevensbescherming (AVG) hebben mensen meer mogelijkheden om voor zichzelf op te komen als hun persoonsgegevens worden verwerkt. Uw systemen, processen en interne organisatie moeten ingericht zijn op deze rechten. Zodat u op de juiste manier gehoor kunt geven aan verzoeken van mensen die hun rechten uitoefenen. U heeft maximaal 4 weken de tijd om te reageren op een verzoek van een betrokkene.AVG art. 78,BRP art 2.53 t/m 2.61
6.2.1.l Heeft de gemeente de betrokkenen over hun rechten geïnformeerd met betrekking tot persoonsgegevens?	Conform AVG artikel 12-14 is een verwerkingsverantwoordelijke (de gemeente) verplicht betrokkenen te informeren over de verwerking van persoonsgegevens. Hij verstrekt aan betrokkene tevens transparante informatie en nadere regels voor het uitoefenen van de rechten van betrokkene.
6.2.3.a Zijn alle benodigde beveiligingsmaatregelen vastgelegd in overeenkomsten met externe partijen?	In overeenkomsten met derden (waaronder samenwerkingsverbanden) waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligingseisen te zijn opgenomen Suwinorm: U.01: de externe partij verstrekt jaarlijks een verklaring aan de afnemer over de aan hen aanbestede diensten in relatie tot Suwinet, zodat afnemer aan zijn/haar assurance verplichtingen kan voldoen. Zie ook hs 6.2.3 van de BIG: Beveiliging behandelen in overeenkomsten met een derde partij p.23Benodigde documentatieContract, SLA, Verwerkersovereenkomst.

Antwoord voor BRP	Score
Meerkeuze: Het College van B&W stelt de informatiebeveiligingsdoelstellingen vast De voortgang wordt jaarlijks besproken tussen B&W en management Er wordt jaarlijks over de voortgang gerapporteerd	100%
Ja	100%
Nee, dit is niet gedetailleerd uitgewerkt	0%
Ja	100%
Ja	100%

Ja	100%
Nee. Er zijn allerhande contacten, maar die zijn niet in beschreven procedures uitgewerkt.	0%
Ja	100%

Ja	100%
Nee	
Nvt ivm antwoord op 6.2.1.a	
Nvt ivm antwoord op 6.2.1.a	
Nvt ivm antwoord op 6.2.1.a	
Nvt ivm antwoord op 6.2.1.a	

Ja	100%
Nvt ivm antwoord op 6.2.1.a	
Nvt ivm antwoord op 6.2.1.a	
Nee. Bij een bestaande applicatie is het niet mogelijk om met terugwerkende kracht "Privacy by Design" toe te passen. Voor nieuwe ontwikkelingen is Privacy uiteraard een belangrijk aandachtspunt	50%
Nee. Bij een bestaande applicatie is het niet mogelijk om met terugwerkende kracht "Privacy by Default" toe te passen. Voor nieuwe ontwikkelingen is Privacy uiteraard een belangrijk aandachtspunt	50%
Ja	100%
Ja	100%
Nvt ivm antwoord op 6.2.1.a	